UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

DECLARATION OF THESIS/ UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's Full Name: LUQMANUL HAKIM BIN MOHD NASIR

Student's Number: 3060007

Title: SECURED AUTONOMOUS AGENT-BASED INTRUSION DETECTION SYSTEM (SAAIDS)

Academic Session: 2 2010/2011

I hereby declare that the work in this thesis/ project paper is my own except for quotations and summaries which have been duly acknowledged.

I acknowledged that Universiti Sains Islam Malaysia reserves the right as follows:

1. The thesis/ undergraduate project paper is the property of Universiti Sains Islam Malaysia.
2. The library of Universiti Sains Islam Malaysia has the right to publish my thesis/ undergraduate project paper as online open access (fulltext) and make copies for the purpose of research or teaching and learning only.

.....
(Student No: 3060007

(Pasport No: 821014-04-5065

Date: 8/3/2011

.....
(Signature of Supervisor)

PROF. DR. KAMARUZZAMAN BIN JEMAN

Date: 8/3/2011

SECURED AUTONOMOUS AGENT-BASED INTRUSION DETECTION SYSTEM (SAAIDS)

LuqmanulHakim Bin Mohd Nasir
(Matric No. 3060007)

Thesis submitted in fulfillment for the degree of
MASTER OF SCIENCE

Faculty of Science and Technology
UNIVERSITI SAINS ISLAM MALAYSIA
NILAI

March 2011

AUTHOR DECLARATION

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: 4th March 2011

Signature:

Name: LuqmanulHakim Bin Mohd Nasir

Matric No: 3060007

Address: No. 2, Lot 14776,
Jalan Sungai Sekamat,
Bt. 12 ½, Jalan Cheras,
43000 Kajang,
Selangor Darul Ehsan.

LuqmanulHakim Bin Mohd Nasir (3060007) was born on the 14th October 1982. He is currently residing at No. 2, Lot 14776, Jalan Sungai Sekamat, Bt. 12 ½, Jalan Cheras, 43000 Kajang, Selangor Darul Ehsan. He previously was a student of UTM and obtained Bachelor of Computer Science from Faculty of Computer Science and Information System. He is at present a Master student of USIM majoring in Information Security.

ACKNOWLEDGEMENT

Praise be upon Allah the Most Gracious Most Merciful for His blessings to enable this completion of research project thesis.

My gratitude goes to my supervisor, Prof. Dr. Kamaruzzaman Seman and my co-supervisor Mrs. Madihah Mohd Saudi for their high dedication, useful guidance and invaluable advices along my research.

I would like to thank Universiti Sains Islam Malaysia (USIM) administration for giving me chances to gain knowledge and experience along my study period. Thanks to Ministry of Science, Technology and Innovation (MOSTI) for their scholarship and grant in ensuring this research is done.

I am most grateful to my parents, Mr. Hj. Mohd Nasir and Mrs. Hjh. Fauziah and my family members for their unlimited prays, love and support. To my beloved wife, Juraida Asna Marhaban and my beloved daughter, Damia Mardhiah for their love, patience and always being there for me. Last but not least, thanks to all my friends and colleagues in USIM and UTM for their unforgotten helps, invaluable guidance, fruitful discussions and ideas about this project.

Thank you.

ABSTRACT

Secured Autonomous Agent-Based Intrusion Detection System (SAAIDS) is developed to design new agent-based intrusion detection system (IDS) based on newly designed SAAIDS architecture and design agent communication and verification protocols and algorithms. The architecture tends to provide secure agent communication and protection of the agent itself. In overcoming problems in existing agent-based IDS, the architecture of SAAIDS is designed to enrol all components in an agent. P2P connection solved single point of failure, multilevel authorization problem and delay on information sending by its design which provides direct connection between agents. In avoiding attacks on message sending process, the architecture was designed with agent communication protocol and algorithm tends to provide secured communication between agents. Agent Verification Protocol and algorithm designed to avoid from unauthorized agent running and doing damages in the system. The unauthorized agent produced when agents being duplicated or altered. The newly designed architecture of SAAIDS, Agent Communication and Verification Protocol and Algorithm was developed and implemented. At the end of the research phase, system testing has proved that the proposed solutions able to avoid all the problems stated above.

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

LIST OF APPENDICES